

Abstract of the Disclosure

A Montgomery modular multiplier receiving a multiplicand (A), a modulus (M), and a multiplier (B), using a t-s compressor, where $t > 3$ and $s > 1$, and a multiplication method performed in the same. In response to a carry propagation adder signal, the t-s compressor performs additions on the carry C and the sum S and obtains the final results in a carry propagation adder structure.